SHOUGANG HIERRO PERÚ S.A.A.
首钢秘鲁铁矿股份有限公司

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

En **Shougang Hierro Perú S.A.A**, (**en adelante SHP**), estamos comprometidos como empresa responsable ante la ley y nuestros trabajadores, en proteger la información personal que nos confían; así como también la data de accionistas, clientes, proveedores, terceros que se relacionen con SHP y la población en general, cumpliendo cabalmente con las disposiciones legales emanadas del Estado Peruano y buscando en todo momento la seguridad y protección de la información.

En el Código de Ética y Conducta de SHP, numeral 14 Protección de Datos, establece como objetivo cumplir con las disposiciones legales y reglamentarias dispuestas por el Estado Peruano en concordancia con las políticas y procedimientos aprobados por SHP como parte de la cultura corporativa y su sistema de prevención.

La protección y seguridad de los datos personales forman parte de nuestra cultura y se fortalece con el cumplimiento y respeto del marco legal establecido por la Constitución Política del Perú y **la Ley de Protección de Datos Personales, Ley N° 29733** (**en adelante la Ley**) y demás normas modificatorias y aclaratorias; así como los convenios ratificados por el Perú sobre la materia.

I. Objetivo:

Establecer los lineamientos de SHP para el cumplimiento de lo dispuesto en el artículo 2, numeral 6 de la Constitución Política del Perú; la Ley de Protección de Datos Personales, Ley N° 29733 sus modificatorias y demás disposiciones reglamentarias como el D.S. N° 016-2024-JUS.

Dicho marco normativo junto a nuestras políticas corporativas constituye la base para garantizar tanto la protección de datos personales albergados en los diferentes bancos de datos de acuerdo a las disposiciones legales, como el ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (Derechos ARCO) que permiten a las personas controlar sus datos personales.

II. Alcance:

La aplicación de la presente Política de Protección de Datos Personales se circunscribe a todos los trabajadores de SHP, sus socios estratégicos, sus directores, sus gerentes, sus accionistas y a todo aquel que actúe en su representación o trabaje dentro de sus instalaciones bajo cualquier modalidad.

La presente Política solo está relacionada a la obtención y tratamiento de datos personales que se utilicen o se encuentren en los bancos de datos de SHP.

En caso de incumplimiento de la presente política, será el Oficial de Protección de Datos Personales quién informe al departamento de Relaciones Industriales para que este determine las sanciones aplicables observando el reglamento interno de trabajo, Código de Ética y Conducta y demás Políticas y procedimientos entre otras disposiciones internas de SHP.

Asimismo, esta política también es aplicable para las empresas proveedoras de bienes y/o servicios, clientes, accionistas, terceros que se relacionen con SHP.

III. Responsabilidad:

La alta dirección y colaboradores de SHP son responsables de la implementación y cumplimiento de la presente Política desde el ámbito de sus funciones y responsabilidades.

El Oficial de Datos Personales de SHP o quien haga las veces de éste, se encargará de asegurar el cumplimiento de la presente Política de acuerdo a las responsabilidades, obligaciones y deberes establecidos en la Ley y sus disposiciones reglamentarias, asimismo, deberá ejercer las siguientes funciones:

- Realizar y actualizar periódicamente el análisis de riesgo y Debida Diligencia sobre dicha materia contando con la participación de las partes responsable involucradas.
- Monitorear la implementación de un Plan de Acción que incluya el manejo de la información y de los diferentes bancos de datos de SHP.
- Canalizar con quien corresponda dentro de SHP las denuncias sobre presunta violación y/o amenaza de transgresión de la Ley de Protección de Datos Personales y demás disposiciones sobre la materia en concordancia con las Políticas y procedimientos de SHP.
- Promover actividades de difusión, sensibilización y capacitación sobre Protección de Datos Personales.

IV. Marco Legal de referencia

- Constitución Política del Perú, artículo 2, numeral 6.
- Ley N° 29733 regula la protección de datos personales. Esta ley establece que los datos personales deben ser veraces, exactos, actualizados, necesarios, pertinentes y adecuados.
- Decreto Supremo N° 016-2024-JUS que deroga el reglamento aprobado por D.S. N° 003-2013-JUS y aprueba el nuevo reglamento de la Ley N° 29733, ley de Protección de Datos Personales.
- Decreto Supremo N° 0029-2021-PCM, Reglamento ley de gobierno digital.
- Resolución Directoral N° 02-2020-JU/DGTAIPD, Directiva para el tratamiento de datos personales mediante Sistemas de Videovigilancia.
- Decreto de Urgencia N° 07-2020, Marco de confianza digital.
- Decreto Supremo N° 0019-2017-JUS, Aprueba el reglamento del decreto legislativo N° 1353, decreto legislativo que crea la autoridad nacional de transparencia y acceso a la información pública, fortalece el régimen de protección de datos personales y la regulación de la gestión de intereses.
- Decreto Legislativo N° 1353, Crea la autoridad nacional de transparencia y acceso a la información pública.
- Resolución Directoral N° 060-2014-JUS/DGPDP, Protección de datos personales en bases de datos personales vinculados con programas sociales.

V. Finalidad del Tratamiento de Datos Personales

Los bancos de datos personales que contengan información de representantes legales, imágenes físicas del personal, exámenes médicos de ingreso a SHP, historias clínicas de los trabajadores de SHP, enfermedades ocupacionales, de compensaciones, beneficios laborales, de accionistas minoritarios, de postulantes, de legajos de personal, de proveedores (personas naturales), de datos de seguridad física y CCTV, de fotocheck (fotografía, huellas dactilares, datos básicos de la persona), padrones de empleo local de relaciones comunitarias y la información de las personas de las comunidades aledañas serán tratados con alguna(s) de la(s) finalidad(es) descrita(s) a continuación:

1. Dar cumplimiento a las obligaciones previstas por la ley; previa coordinación o consulta con la Autoridad de Datos Personales.
2. Contar con un registro de los exámenes médicos ocupacionales, del personal de SHP y contratistas de acuerdo a lo requerido por la Ley de Seguridad y Salud en el Trabajo, o la norma vigente relacionado a los mismos temas.
3. Contar con un registro de las historias clínicas del personal de SHP y contratistas que reciben servicios de salud en el puesto de salud de la zona donde se encuentran ubicadas nuestras operaciones.
4. Mantener un registro de los representantes legales de SHP para fines corporativos y de gestión.
5. Contar con la información relacionada a las enfermedades ocupacionales de los trabajadores de SHP y personal de contratistas que prestan servicio para SHP.
6. Contar con información relacionada al registro de información personal y laboral del trabajador para la adecuada gestión del área de recursos humanos de SHP, y cumplimiento de las obligaciones y compromisos dinerarios de acuerdo a Ley y los procedimientos internos de SHP.
7. Contar con un Registro o Padrón ordenado de accionistas de SHP y sus valores.
8. Contar con un registro para el control de la información que se obtiene como consecuencia del manejo de datos de contacto de los candidatos a distintas posiciones vacantes en SHP.
9. Contar con un banco de datos con el registro de información personal del trabajador para la adecuada gestión del área de Recursos Humanos.
10. Contar con un registro ordenado de los proveedores de SHP.
11. Contar con un registro único y ordenado en donde se registren el control de accesos, salidas y seguridad en la mina y otras instalaciones de SHP.
12. Contar con un registro único de acreditaciones de personal para control de accesos.
13. Efectuar el pago de salarios, prestaciones sociales, indemnizaciones y aportes a la seguridad social y los procesos operativos inherentes a ello;
14. Afiliación del suscrito y de su familia a las entidades que forman parte del plan de compensación, médico o cualquier otro previsto por Ley;
15. Suministrar información que pueda ser de interés del titular de datos personales
16. Envío de la información recibida a empresas vinculadas (información sobre nómina, compensaciones, etc.), acreditando la seguridad de los parámetros de seguridad de quien recibirá los Datos Personales.
17. Administración interna de información sobre capacitaciones, cursos y evaluaciones de desempeño.

18. Realizar actividades propias de Recursos Humanos y de Seguridad y Salud Ocupacional, que sean estrictamente necesarias para llevar a cabo la relación laboral.
19. Proporcionar información que pueda ser de interés del trabajador;
20. Cuando SHP lleve a cabo las actividades requeridas para desarrollar su objeto social.
21. Otras finalidades necesarias que permitan, velar por el cumplimiento de la Ley de Protección de Datos Personales, para los cuales SHP tiene el consentimiento para tratar.

Las finalidades señaladas en el párrafo que antecede son meramente enunciativas más no limitativas, y por tanto SHP podrá modificar o aumentar sus bancos de datos para el tratamiento adecuado conforme a la Ley y exigido por la autoridad competente.

VI. Principios

La actuación de los titulares de los datos personales, el Oficial de Protección de Datos Personales o quien haga sus veces y los encargados de los bancos de datos personales, así como de quien resulte responsable del tratamiento y, en general, de todos los que intervengan en relación a datos personales, y el registro o administración de los mismos, debe regirse por los siguientes principios rectores establecidos en las disposiciones legales pertinentes y sus respectivos reglamentos.

En este sentido, SHP considera como principios de la Política de Protección de Datos Personales, lo siguiente:

Principio de consentimiento: El tratamiento de datos personales por SHP, será lícito cuando el titular de los datos personales, preste su consentimiento libre, previo, expreso, informado e inequívoco. No se admite el consentimiento por presunción.

Principio de finalidad: El tratamiento de datos personales debe obedecer a una finalidad determinada, explícita y lícita, la que deberá ser informada previamente al titular de los datos personales. Dicho tratamiento no debe extenderse a otra finalidad que no haya sido la establecida.

Tratándose de datos sensibles, SHP podrá almacenar los mismos en un banco de datos, cuando su finalidad, además de ser legítima, sea acorde con sus actividades o fines explícitos.

Los profesionales a quienes SHP encargue el tratamiento de algún dato personal, deberán limitarse a cumplir con la finalidad de sus servicios, además de encontrarse obligados a guardar secreto profesional.

Principio de proporcionalidad: Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que han sido recopilados.

Principio de calidad: Los datos personales a tratar deben ser veraces, exactos y, en la medida de lo posible; actualizados, necesarios, pertinentes y adecuados respecto de la

finalidad para la que fueron recopilados. Deben conservarse de forma tal que se garantice su seguridad y por el tiempo necesario para cumplir con su finalidad.

Principio de seguridad: La información sujeta a tratamiento por SHP, se debe manejar con las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales, a fin de evitar cualquier tratamiento, intencional o no, contrario a las normas de protección de datos personales, incluyéndose en ellos la adulteración, pérdida, desviaciones de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Asimismo, las medidas de seguridad adoptadas por SHP deben ser apropiadas en relación al tratamiento que se va a efectuar y a la categoría de datos que se trate.

Principio de transparencia: El tratamiento de datos personales debe ser informado de manera permanente, clara, fácil de entender y accesible al titular de los datos personales. SHP pondrá a conocimiento del titular dato personal, las condiciones del tratamiento de sus datos personales, así como de los derechos que puede hacer valer respecto a aquellos y de las demás condiciones establecidas en el artículo 18 de la Ley.

Principio de responsabilidad proactiva: En el tratamiento de datos personales se deben aplicar las medidas legales, técnicas y organizativas a fin de garantizar el cumplimiento efectivo de la normativa de datos personales, y el titular del banco de datos personales o quien resulte responsable, debe ser capaz de demostrar tal cumplimiento.

VII. Glosario de Términos y Definiciones

Para efecto de la aplicación de los presentes lineamientos se establecen las siguientes definiciones:

1. **Banco de datos personales:** Es el conjunto de datos de personas naturales computarizado o no, y estructurado conforme a criterios específicos, que permita acceder sin esfuerzos desproporcionados a los datos personales, ya sea aquel centralizado, descentralizado o repartido de forma funcional o geográfica.
2. **Bloqueo:** Es la medida que consiste en la identificación y reserva de los datos personales adoptando medidas técnicas y organizativas para impedir su tratamiento, incluyendo su visualización, durante el periodo en que se esté procesando alguna solicitud de actualización, inclusión, rectificación o supresión, en concordancia con lo que dispone el tercer párrafo del artículo 20 de la Ley. Se dispone también como paso previo a la cancelación por el tiempo necesario para determinar posibles responsabilidades en relación a los tratamientos durante el plazo de prescripción legal o prevista contractualmente.
3. **Cancelación:** Es la acción o medida que en la Ley se describe como supresión, cuando se refiere a datos personales, que consiste en eliminar o suprimir los datos personales.
4. **Datos personales:** Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, de localización, identificadores en línea o de cualquier otro tipo concerniente a aspectos físicos, económicos, culturales o sociales de las personas naturales que las identifica o las hace identificables. Se considera identificable cuando se puede verificar la identidad de la persona de manera directa o

indirectamente a partir de la combinación de datos a través de medios que puedan ser razonablemente utilizados.

5. **Datos personales relacionados con la salud:** Es aquella información concerniente a la salud pasada, presente o pronosticada, física o mental, de una persona, incluyendo la información que se derive de un acto médico, el grado de discapacidad y su información genética.
6. **Datos sensibles:** Es aquella información relativa a datos genéticos o biométricos de la persona natural, datos neuronales, datos morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la afiliación sindical, salud física o mental u otras análogas que afecten su intimidad.
7. **Desindexación:** Es el proceso mediante el cual una dirección URL o contenido específico de un sitio web es eliminado o excluido de los resultados de motores de búsqueda. Este procedimiento, dependiendo de la situación y las circunstancias específicas, puede ser efectuado por el propietario del sitio web o por el motor de búsqueda.
8. **Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales:** Es el órgano encargado de ejercer la Autoridad Nacional de Protección de Datos Personales a que se refiere el artículo 32 de la Ley, pudiendo usarse indistintamente cualquiera de dichas denominaciones en el presente Política.
9. **Encargado de tratamiento de datos personales:** Es la persona natural, persona jurídica de derecho privado o entidad pública que realiza tratamiento de datos por cuenta u orden del responsable de tratamiento o titular del banco de datos personales.
10. **Elaboración de perfiles:** Es la forma de tratamiento automatizado de datos personales que permite evaluar aspectos de una persona natural, de manera específica y continua, para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamientos o hábitos, ubicación o movimientos.
11. **Emisor o exportador de datos personales:** Es el titular del banco de datos personales o aquel que resulte responsable del tratamiento de dichos datos, situado dentro del territorio nacional y que realiza una transferencia de datos personales a otro país, conforme a lo dispuesto en el presente Política.
12. **Evaluación de impacto relativo a la protección de datos personales:** Es el mecanismo de responsabilidad proactiva que consiste en que el titular del banco de datos personales o responsable del tratamiento de datos realice, de forma previa al tratamiento de los mismos, un análisis o evaluación del impacto o riesgos que implica el tratamiento de esos datos.
13. **Fines de tránsito:** Implica que los medios no son usados para la finalidad específica de realizar el tratamiento de datos personales, tales como procesamiento, almacenamiento, descarga, visualización y/o similares, sino exclusivamente para hacer pasar datos personales de un lugar a otro.
14. **Flujo transfronterizo de datos personales:** Se denomina flujo transfronterizo o transferencia internacional de datos personales a la transferencia de datos personales a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte en que estos se encuentren, los medios por los cuales se efectuó la transferencia ni el tratamiento que reciban.
15. **Incidente de seguridad de datos personales:** Es toda vulneración de la seguridad

que ocasione la destrucción, pérdida, alteración ilícita de los datos personales o la comunicación o exposición no autorizada a dichos datos.

16. **Oficial de Datos Personales:** Es la persona designada por el responsable de tratamiento o encargado del tratamiento de datos personales para la verificación, asesoramiento e implementación del cumplimiento del régimen jurídico sobre protección de datos personales.
17. **Receptor o importador de datos personales:** Es toda persona natural o jurídica de derecho privado, incluyendo las sucursales, filiales, vinculadas o similares o entidades públicas, que recibe los datos en caso de transferencia internacional, ya sea como titular del banco de datos personales o encargado del tratamiento.
18. **Rectificación:** Es aquella acción destinada a afectar o modificar un dato personal ya sea para actualizarlo o corregirlo con datos exactos.
19. **Representante:** Es la persona natural o jurídica designada de manera expresa, por el titular del banco de datos personales o responsable, para fines del tratamiento de datos personales.
20. **Repertorio de jurisprudencia:** Es el banco de resoluciones judiciales o administrativas, dictámenes fiscales, laudos arbitrales, resoluciones de comités de ética o similares, que se encuentra en soporte físico o digital, y organiza, entre otros, datos personales como fuente de consulta y habitualmente pública.
21. **Responsable del tratamiento:** Es la persona natural, persona jurídica de derecho privado o entidad pública que decide sobre la finalidad y medios del tratamiento de datos personales. Esta definición no se restringe al titular del banco de datos, sino que incluye a cualquier persona que decida sobre el tratamiento de datos personales, aun cuando no se encuentre en un banco de datos personales.
22. **Tratamiento:** Es cualquier operación o conjunto de operaciones, automatizados o no, que se realicen sobre los datos personales o conjuntos de datos personales.

VIII. Derechos del Titular de Datos Personales

El titular de los datos personales tendrá los siguientes derechos frente al tratamiento de los mismos:

a) Derecho a ser informado oportunamente por SHP, de manera detallada, sencilla, expresa, inequívoca y previa a la recopilación de sus datos personales, sobre: (i) la(s) finalidad(es) de su tratamiento; (ii) sus destinatarios,(iii) el banco de datos en que se almacenarán, así como la identidad y domicilio de su titular y, de ser el caso, del encargado del tratamiento de sus datos personales; (iv) el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles; (v) la transferencia de los datos personales; (vi) las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; (vii) el tiempo de conservación de sus datos personales; (viii) y la posibilidad de ejercer los derechos que la ley le concede y los medios previstos para ello.
b) Derecho a ejercer personalmente o mediante su representante o apoderado, previa acreditación de identidad, los derechos de acceso, rectificación, cancelación y oposición.
c) Derecho a revocar su consentimiento, en cualquier momento, para el tratamiento de sus datos personales, ya sea para todas las finalidades que consintió o para alguna(s) de ellas.

d) Derecho a impedir y/o suspender que sus datos personales sean suministrados, salvo las excepciones previstas en leyes aplicables.
e) Goza de la libertad de recurrir, cuando considere necesario, a la Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP) o al Poder Judicial cuando se deniegue el ejercicio de sus derechos, así como reclamar la indemnización correspondiente cuando se vea afectado a consecuencia de dicho incumplimiento.

IX. Obligaciones y Responsabilidades del Titular de Banco de Datos Personales

SHP, en calidad de titular y responsable de los bancos de datos personales que registre, deberá cumplir con las siguientes obligaciones enunciativas, más no limitativas:

a) Debe obtener el consentimiento libre, previo, informado, expreso e inequívoco del titular de datos personales para el tratamiento de sus datos personales con fines específicos.
b) Debe informar de manera clara y detallada, al titular de datos personales, la(s) finalidad(es) del tratamiento de sus datos.
c) Debe garantizar y NUNCA recopilar u obtener datos personales por medios fraudulentos, desleales o ilícitos.
d) Debe recopilar datos personales que sean actualizados, necesarios, pertinentes y adecuados, con relación a finalidades determinadas, explícitas y lícitas para las que se hayan obtenido.
e) Debe verificar la capacidad legal del titular de los datos. Caso contrario, los datos personales de menores de edad deberán ser tratados de acuerdo con lo indicado en la sección especifica indicada en al apartado XI de la presente Política.
f) Debe velar y garantizar el uso adecuado de los datos personales con los fines específicos y evitar su uso con propósitos o finalidades distintas a aquellas que motivaron su obtención, salvo que medie procedimiento de anonimato o de separación.
g) Debe Suprimir, sustituir y/o completar los datos personales objeto de tratamiento cuando tenga conocimiento de su carácter inexacto o incompleto, sin perjuicio de los derechos del titular al respecto.
h) Debe Suprimir los datos personales objeto de tratamiento cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hubiesen sido recopilados o hubiese vencido el plazo para su tratamiento, salvo que medie procedimiento de anonimato o de separación.
i) Debe proporcionar a la Autoridad de Protección de Datos Personales la información relativa al tratamiento de datos personales que esta le requiera, así como consultar en caso será requerido por autoridad distinta o terceros.

SHP debe aplicar los plazos de retención de información que contenga datos personales según las leyes especiales que los regulen.

X. Tratamiento de Datos Personales de Menores

La autorización del tratamiento de los datos personales de un menor de edad, se realizará con el consentimiento de los titulares de la patria potestad o tutores, según corresponda.

NO son válidos los consentimientos otorgados por los propios menores de edad para acceder a actividades vinculadas con bienes o servicios que están restringidos para mayores de edad, ni para obtener información sobre sus familiares, a excepción de los datos de identidad y dirección de los padres o tutores con la finalidad de obtener el consentimiento de los mismos.

De acuerdo a la Ley y de manera excepcional, el adolescente mayor de catorce años y menor de dieciocho años podrá otorgar, por sí mismo, su consentimiento para el tratamiento de sus datos personales, siempre que la información proporcionada haya sido expresada en un lenguaje claro y sencillo, que permita ser comprensible por ellos.

XI. Tratamiento de Datos Sensibles

De acuerdo con las disposiciones legales sobre Protección de Datos, para el tratamiento de datos sensibles, SHP deberá obtener el consentimiento por escrito, a través de la firma manuscrita, digital o cualquier otro mecanismo de autenticación, que garantice la voluntad inequívoca del titular. No será necesario el consentimiento del titular, únicamente cuando la Ley lo autorice por motivos importantes de interés público.

XII. Transferencia y flujo transfronterizo de Datos Personales

Como parte del desarrollo de sus actividades, SHP podrá efectuar transferencias de datos personales de los titulares de acuerdo a la Ley y las disposiciones internas de SHP.

En el caso de las transferencias de datos personales entre las sedes en Perú y China, se deberá cumplir con garantizar el tratamiento de datos personales de acuerdo a las disposiciones legales, políticas y procedimientos internos de SHP.

Para el flujo transfronterizo de datos personales, SHP tomará las medidas necesarias para que los receptores conozcan y se comprometan a observar la presente Política, así como lo establecido por la Ley, su Reglamento y demás disposiciones sobre la materia. Quienes reciban la información asumirán las mismas obligaciones que corresponden al titular del banco de datos personales o responsable del tratamiento, que como emisor o exportador transfirió los datos personales y sólo podrán utilizarla para asuntos directamente relacionados con SHP. Para dichos efectos, SHP podrá hacer uso de cláusulas protectoras contractuales u otros instrumentos jurídicos en los que se establezcan, mínimamente, las mismas obligaciones a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales.

XIII. Garantía y Seguridad de los Datos Personales

SHP hace de conocimiento que las medidas y mecanismos utilizados para tratamiento de datos personales cumplen con las exigencias legales y necesarias para garantizar la seguridad y confidencialidad de los datos personales que se administran.

XIV. Vigencia

La presente Política de Protección de Datos Personales, entrará en vigencia a partir de la aprobación, por parte del Directorio de SHP; y será difundida a todo el personal de SHP a través del portal web de SHP al cual tienen acceso todos los trabajadores y personas en general.

XV. Aprobación y Actualización de la Política

La presente Política de Protección de Datos Personales será aprobada por el Directorio de SHP y actualizada cada vez que exista un cambio significativo en las condiciones internas y ~~externas~~, cambios normativos e innovaciones en las prácticas de tratamiento de datos personales con el propósito de garantizar el tratamiento legal y seguro de los datos personales existentes en nuestros bancos de datos Personales.